Incrementando la detección de Incidentes Informáticos

Selección e Implementación de herramientas de detección de incidentes.

Cena, Norberto Gaspar

Mussetta, Sebastián Norberto

Córdoba, Fernando Martín

Belamate, David Jesús

Favro, Ignacio Daniel

Cassani, Matías Alberto

Universidad Tecnológica Nacional, Facultad Regional Villa María

Abstract

Dado el continuo y vertiginoso avance de la tecnología de la información, los administradores de servicios informáticos de red deben ocuparse cada vez más de la seguridad de la Información. De manera continua, nuevas vulnerabilidades de software son detectadas y explotadas mediante diferentes técnicas de intrusión a los Sistemas de red cliente-servidor. A menudo, los servicios informáticos no son protegidos de manera adecuada debido al continuo cambio en las técnicas de acceso no autorizado a la Información. El presente trabajo tiene como objetivo, determinar a través de servicios publicados en ambientes informáticos controlados, los mecanismos de ataques actuales, vulnerabilidades de servicios y la generación de políticas de seguridad que permitan la protección de acceso no autorizado a la información. Los servicios como web, correo, bases de datos, proxies, ssh, etc., fueron publicados en la red en un ambiente de virtualización controlado, a modo de honeypot. Los honeypot son servicios informáticos con configuraciones predeterminas, o con políticas de seguridad poco robustas, que facilitan el acceso a la información por parte de intrusos, para poder realizar un estudio detallado de las técnicas de intrusión utilizadas, impacto del incidente de seguridad, vulnerabilidad explotada, etc. El estudio del incidente informático se realiza a través del seguimiento de los registros logs de los servicios en cuestión. Varios de los servicios de red publicados han sido vulnerados por medio de diferentes mecanismos de generación de incidentes. El estudio de los incidentes permitió contribuir a la generación de políticas de seguridad en el sistema de producción.

Palabras Clave

Seguridad, informática, incidente, honyepot, redes, servicios, detección, vulnerabilidad, ataque, intrusión.

Introducción

La seguridad informática es una preocupación creciente para las organizaciones e individuos, esto a llevado a un creciente interés en las formas más agresivas de defensa para complementar los métodos existentes. Uno de estos métodos implica el uso de honeypots. Un honeypot es un recurso de seguridad cuyo valor radica en ser investigado, atacado o comprometido [1].

"Un honeypot es un recurso del sistema de información cuyo valor reside en el uso no autorizado o ilícito de esos recursos" [2]

Los usuarios confiables que conocen la organización interna tienen como objetivo acceder a la información de los sistemas y no a los sistemas en sí.

Cuando protegemos una red, se deben usar tres tipos de sistemas de seguridad juntos, primero se emplean elementos de seguridad estructurales como Firewalls, en segundo lugar es necesario monitorear el tráfico de la red, y finalmente debería haber una opción para reaccionar ante cualquier tipo de amenaza [3].

Las Honeypots son utilizadas para detectar, identificar y reunir información sobre amenazas específicas de la infraestructura informática de una Organización. La implementación de un honeypot proporciona una capacidad sin precedentes a los administradores de redes informáticas para protegerse de ataques informáticos. Litzner define los honeypots como una herramienta de seguridad cuyo valor radica en ser investigada, atacada o comprometida [4]. En otras palabras están son sistemas de computación, altamente monitoreados con el propósito de atraer a los hackers, analizar su modus operandi y el perfil de ellos [5].

Niels Provos introduce dos tipos de honeypots: los honeypots de alta interacción que implican el despliegue de sistemas operativos reales en honeypots de interacción real o máquinas virtuales. Y los honeypots de baja interacción que son programas informáticos emulando sistemas operativos y servicios [6].

Con el avance del tiempo y a medida que la tecnología de las comunicaciones fue creciendo, las organizaciones, cada vez con más frecuencia, permiten a las personas acceder a sus sistemas a través de redes informáticas. Transacciones bancarias, compras por Internet, Correos Electrónicos, Sistemas de Autogestión, Sistemas de Reclamos, etc. son ejemplos comunes de

este tipo de interacción entre personas fuera de la organización y sistemas de información a través de redes públicas. Por otro lado los usuarios móviles que pertenecen a las organizaciones necesitan a menudo acceder a sus sistemas por medio de dispositivos móviles utilizando redes públicas y privadas.

Los productos de software, tales como los servicios de red, se van actualizando rápidamente adquiriendo nuevas características y funcionalidades, pero además es muy probable que incorporen también en dichos cambios, nuevas vulnerabilidades que puedan ser explotadas por atacantes dentro o fuera de la red local.

A menudo, en todos estos sistemas, se generan incidentes de seguridad en la información donde intrusos (personas o programas) intentan acceder de manera no autorizada a dicha información. Muchas veces estos ataques son exitosos generando problemas tales como: acceso a información confidencial, pérdida de datos, denegaciones de servicios, entre otros.

Con el desarrollo de este proyecto se interpretarán diversos tipos de ataques a la información mediante la utilización de diferentes tipos de honeypots. Los honeypots son programas que simulan diferentes servicios de red tales como web, correo, proxys, ssh, dns, firewalls, etc en producción con vulnerabilidades de manera que los atacantes se sientan tentados a explotar. Frecuentemente, dichas vulnerabilidades son conocidas, ya que han sido publicadas previamente pero otras veces no se conocen. Esta información es de vital importancia para la generación de una correcta política de seguridad de la información en la organización. Una Política de Seguridad es una expresión formal de reglas que deben cumplir aquellas personas que tienen acceso a información y tecnologías de una organización [7].
La política de seguridad puede observarse como el centro de una rueda en el que giran actividades que interactúan con el centro: Asegurar, controlar, probar y mejorar [8]. La utilización de honeypots contribuye a la definición de una política de seguridad.

Todos estos ataques son registrados dentro de los honeypots en forma de registros logs para que los administradores puedan estudiar y tomar acciones proactivas en los servicios disponibles de las redes informáticas de las organizaciones. Un ambiente de virtualización en la infraestructura Informática de la Universidad Tecnológica Nacional Facultad Regional Villa María, fue implementado en el presente trabajo para realizar un mejor aprovechamiento y reutilización del hardware disponible, donde diversos Sistemas Operativos y aplicaciones de red comparten el hardware en el que son ejecutados.

Elementos de Trabajo y metodología

El desarrollo del trabajo de investigación se realizó utilizando la infraestructura informática de la Universidad Tecnológica Nacional Facultad Villa María. La misma cuenta con equipamiento informático de última generación incorporando tecnologías como fibra óptica, redes virtuales (vlans), subredes, cableado estructurado, etc. La red del Campus Universitario de la Regional Villa María brinda diferentes servicios de red a su comunidad Académica tales como Web, Campus Virtual, Correo Electrónico, Ftp, Vpn, Proxy, Internet, entre otros. La mayoría de los servicios brindados son comúnmente utilizados por diferentes organizaciones educativas, gubernamentales, comerciales, ya sean públicas o privadas. Para poder brindar un servicio adecuado el administrador de red debe implementar una política de seguridad apropiada, de manera que se impida el acceso no autorizado a la información de valor de los sistemas de la organización. Resulta necesario, para definir esta política, conocer las diferentes vulnerabilidades de los sistemas de información, así como también los diversos mecanismos de ataques y generación de incidentes

informáticos que pueden ser originados, tanto dentro, como fuera de la Organización. Debido a esto, se implementó una plataforma de honeypots con servicios comúnmente utilizados en la organización para lograr efectuar un seguimiento de intentos de acceso no autorizado a la información, pudiendo realizar un tracking (seguimiento) de los incidentes de seguridad detectados. Esta información es la que permitió generar nuevas políticas de seguridad para aplicar en la organización, actualizando versiones de software, aplicando nuevas reglas de firewalls, modificando configuraciones de sistemas, entre otras.

A continuación se describen las etapas que se fueron cumpliendo durante la realización del presente trabajo:

1) Definición de la Arquitectura de soporte a Sistemas Operativos y Servicios

En esta instancia se evaluó la posibilidad de utilizar diferentes plataformas de Virtualización para optimizar el rendimiento y administración del hardware disponible. El grupo de investigación poseía equipos de tipo clon Intel Core 2 Duo con gabinetes rackeables para la instalación de la infraestructura honeypots, en un ambiente de prueba aislado del entorno de producción. Las plataformas de virtualización viables para la puesta en marcha de la infraestructura poseían como requisito principal soportar hardware no Homologado, ya que los equipos eran de tipo clon. Entre las opciones de virtualización se evaluó la posibilidad de instalar la plataforma directamente sobre el disco rígido funcionando como Sistema Operativo o instalar un Sistema Operativo sobre el disco y la plataforma en el Sistema Operativo en cuestión. Finalmente se resolvió la instalación de VMware Workstation 9 sobre Debian GNU/Linux.

2) Definición de Sistemas Operativos y Servicios

Durante el desarrollo de esta fase, se determinaron los Sistemas Operativos y Servicios a utilizar en modo honeypots. Además, se evaluó la posibilidad de implementar soluciones Honypots ya desarrolladas tales como Honeyd, Kippo, etc.

Para determinar los Sistemas Operativos y servicios de red se optó por utilizar tanto SO como servicios que se encuentran en producción la Universidad Tecnológica Nacional Facultad Regional Villa María.

Los Sistemas Operativos que se instalaron en diferentes máquinas virtuales fueron: Debian GNU/Linux 6.0 y Microsoft Windows 2003 Server.

Los servicios de red que se detallan a continuación fueron instalados en modo honeypot en los Sistemas Operativos nombrados anteriormente: Squid Proxy Cache 3.3, Ssh, Postfix 2.9, Qmail 1.0.5, Apache Web Server 2.2, Internet Information Server, Postgresql 8.2.2, Mysql 5.5, Joomla 2.5.

Kippo 0.5 es un honeypot que simula un servidor ssh, que permite capturar y registrar la interacción del atacante en un registro log de manera automática. Kippo fue implementado en Debian GNU/Linux 6.0 en este proyecto.

3) Distribución de los servicios, servidores y Hardware

Dos equipos de computación de tipo clon, instalados en gabinetes rackeables, fueron utilizados como soporte de hardware en el desarrollo de este proyecto. Los mismos poseen las siguientes características: Procesador Intel Core 2 Duo, Disco Rígido de 160 gb, Memoria Ram 2Gb. En ambos equipos de hardware se instaló Debian Linux 6.0 y VMware Workstation 9.0.

La siguiente tabla muestra un resumen de las características de Hardware y la distribución de software base durante este proyecto.

	Servidor 1	Servidor 2
Procesador	Intel Core 2 Duo	Intel Core 2 Duo
Disco Rígido	160 Gb	160 Gb
Memoria Ram	2 Gb	2 Gb
SO Base	Debian Linux 6.0	Debian Linux 6.0
Virtualización	VMware	VMware
Imagen		

Tabla 1. *Descripción de Hardware de Servidores*

En la plataforma de VMware del servidor 1 se instalaron dos Servidores Debian Linux 6.0. En el primer servidor se instalaron los siguientes servicios: Postgresql 8.2.2, Myslq 5.5 y kippo 0.5. En el segundo servidor se instaló Apache 2 Web Server, Joomla 2.5, Squid-Cache 3.3., Ssh

En la plataforma de VMware del servidor 2 se instaló un Servidor Debian Linux 6.0 y un servidor Ms Windows 2003 Server.

En el Servidor Debian Linux 6.0 del VMware 2 se instalaron los siguientes servicios: Postfix 2.9, Qmail 1.0.5, Ssh y en el Servidor Ms Windows 2003 se instaló Server IIS (Internet Information Server) y MS SQL Server.

Las siguientes tablas muestran un resumen de la distribución de Servicios de red y Sistemas Operativos utilizados durante este proyecto.

Debian Linux 6.0	Debian Linux 6.0
Postgresql	Apache Web Server
Mysql	Joomla
Kippo	Squid-cache
	Ssh

Tabla 2. *Servicios del Servidor 1*

Debian Linux 6.0	Ms Windows 2003
Postfix	IIS
Qmail	Ms SQL Server 2000
Ssh	

Tabla 3. *Servicios del Servidor 2*

4) Estrategias de configuración de Sistemas Operativos y Servicios de red

Ups (Uninterruptible Power Supply): Instalación de una unidad ups a los servidores físicos para protegerlos de interrupciones en el suministro eléctrico.

Acceso a los Sistemas Operativos Base: el acceso a la administración de los sistemas operativos base de soporte a VMware Workstation se realizó a través de los servicios VNC y SSH.

Configuración de los Sistemas Operativos Base: ambos sistemas operativos base en los servidores físicos han sido configurados con un correcto hardening del Sistema. Algunas de las políticas de seguridad aplicadas fueron las siguientes: políticas de firewall, iptables en drop por defecto, sólo permitiendo el tráfico deseado como por ejemplo vnc, ssh, ntp, entre otros. Limitación de cantidad de conexiones simultaneas por cliente a nivel firewall ("iptables") para evitar ataques de DoS (Denegación de Servicios) Ej.syn flooding. Limitación de acceso por ssh al usuario root. Privación de ejecución de shell (/bin/bash) a determinados usuarios. Se consideró necesario aplicar un correcto hardening de ambos sistemas operativos base para minimizar y prevenir riesgos de ataques que puedan afectar las máquinas virtuales que en ellos se ejecutaban.

Servidor de tiempo (ntp): se consideró muy importante la instalación de un servidor de tiempo ntp dentro de la granja de servidores virtualizados. Este servicio permite que todos los relojes de los Sistemas Operativos clientes se encuentren sincronizados. Esta sincronización de relojes sirve para poder realizar un correcto seguimiento del incidente de seguridad en caso que el mismo sea originado. De esta manera el administrador puede determinar la cronología de los eventos de los sistemas en los diferentes servidores afectados.

Nivel de detalle de logs: se configuraron los diferentes Sistemas Operativos y Servicios de red para que registren la mayor cantidad de detalle en los archivos logs. Por defecto,

muchos servicios y servidores no guardan suficiente nivel de detalle en los registros de eventos log. Esto hace que el administrador de red no cuente con suficiente información para realizar un correcto seguimiento de incidentes.

Direccionamiento: los servidores virtualizados fueron configurados con direcciones IP públicas dentro del rango de direcciones disponibles de la UTN FRVM. Los demás servidores de la red en producción se encuentran en DMZ, detrás de firewall que impide los accesos desde los servidores virtuales.

Configuración de Servicios y Servidores virtuales: Se crearon las máquinas virtuales en VMware y se instalaron los sistemas operativos virtuales. El hardware de las máquinas virtuales se configuró acorde a los requerimientos de Sistemas Operativos y servicios a instalar. Luego se instalaron los diferentes servicios en las Sistemas Operativos Virtuales. En general, se establecieron las configuraciones de los SO virtuales y servicios por defecto.

- Servidores Virtuales Debian Linux: políticas de firewall (iptables) por defecto en Accept. Usuarios de sistemas con permiso de ejecución de shell. Permiso de acceso por ssh al usuario root.
- Servidor Virtual Ms Windows 2003 Server: instalación por defecto con Service pack II y actualizaciones automáticas configuradas.
- Postgresql 8.2.2: configurado para que escuche (Listen) en todas las interfaces de red Tcp Puerto 5432 (Por defecto). Contraseña de usuario postgresql poco robusta. Creación de base de datos para los servicios Apache, Joomla, Postfix.
- Mysql 5.5: configurado para que escuche (Listen) en todas las interfaces de red. Puerto Tcp 3306 (Por defecto). Contraseña de usuario mysql poco robusta. Creación de bases de datos para el servicio Qmail y Kippo.
- Ssh: instalación por defecto. Permiso de acceso a usuario root. Configurado para que escuche (Listen) en todas las interfaces de red Tcp Puerto 22 (Por defecto).
- Kippo 0.5: honeypot que simula el servicio ssh. Configuración por defecto.
- Apache 2: Instalación con soporte php, postgresql, mysql. Se configuraron varios dominios virtuales con sitios webs, con acceso a bases de datos postgresql y mysql, envío de correo electrónico y formularios online. Configuración básica php: memory_limit =128M, register_globals=on, max_upload_size = 10M, magic_quotes, entre otras.
- Joomla 2.5: Sistema de gestión de contenido Web CMS (Content Management System), que permite desarrollar sitios web de manera dinámica a través de un panel de control amigable. Instalación por defecto. Desarrollo de sitio web utilizando las características básicas del servicio. Formulario dinámico, acceso a documentos, Galerías de imágenes, calendarios, servicios de suscripción, boletines de noticias, foros y chats, entre otros.
- Squid 3.3 proxy cache: Instalación por defecto. configurado para que escuche (Listen) en todas las interfaces de red. Puerto Tcp 3128 (Por defecto).
- Postfix 2.9: Instalación básica por defecto con Spamassasin y clamav. Configuración de un dominio virtual. Autenticación plana. Usuarios virtuales dentro de base de datos postgresql. Administración por medio de Isoqlog.
- Qmail: Instalación básica por defecto con Spamassasin y clamav. Configuración de un dominio virtual. Autenticación plana. Usuarios virtuales dentro de base de datos mysql. Administración por medio de Isoqlog.
- IIS: Configuración básica por defecto.Configurado para que escuche (Listen) en todas las interfaces de red Tcp Puerto 80 y 443 (Por defecto).

Creación de sitio web desarrollado en Asp con acceso a Ms SqlServer 2000.

- Ms SqlServer 2000: configuración por defecto. Creación de base de datos para acceso desde Sitio Asp en IIS.

5) Configuración de herramientas útiles

Una vez instalados los servicios nombrados anteriormente, se procedió a la instalación de un conjunto de herramientas que contribuyeron a la administración y monitoreo de los servicios. Por otro lado sirvió para definir una línea base de comportamiento de los servicios de red en cuestión. Las herramientas utilizadas son:

Postfixadmin 2.3.6: herramienta web que facilita la administración de las cuentas de usuario de correo, dominios virtuales de correo, entre otras.
Isoqlog 2.2.1: herramienta web que permite ver estadísticas de la utilización de los servicios Postfix y Qmail. Ej.: cantidad de correos enviados y recibidos por cuenta de correo, por dominio, volumen de información transferida por correo electrónico, entre otras.
Nagios 3.3.1: herramienta con soporte web utilizada para el monitoreo del estado de servidores y servicios. Configuración de alertas de correo electrónico.
Cacti 0.8.8a: herramienta con soporte web para el monitoreo de servidores por medio del protocolo Snmp. Ej.: cantidad de usuarios logueados, consumo de CPU, disco y memoria, tráfico de tx y rx de las interfaces de red, entre otras.
Sarg 2.3.3: herramienta con soporte web que genera reportes de tráfico http. A través de un parser del archivo access.log del servicio Squid genera un sitio web con los reportes de tráfico por ip, dominio, hora, entre otros.
Postfix Server Activity Summary: esta herramienta envía un correo resumen diario con las estadísiticas del servidor de correo Postfix.
Logwatch 7.3.5: esta herramienta envía un correo resumen diario con las estadísiticas de diferentes servicios.
Qmail-mrtg 7.4.2: esta herramienta grafica en la web las estadísticas del servidor de correo Qmail.

Resultados

Los resultados obtenidos en el presente trabajo fueron satisfactorios. Los servicios publicados sufrieron diferentes tipos de ataques informáticos generando diversos incidentes de seguridad en los honeypots de manea exitosa. Los sistemas Operativos Debian Linux 6.0 base no sufrieron ataques. Todos estos incidentes fueron estudiados y permitieron a los administradores de la red construir políticas de seguridad en la red en producción. Nuevas reglas de firewalls, correcto hardening de los diferentes servicios de red, cambio de productos de software, son algunas de las medidas tomadas por los administradores de la red en producción luego de este trabajo.
A continuación se realizará un detalle de los incidentes registrados en los diferentes honeypots.
La honeypot Kippo sufrió ataques de fuerza bruta. Todos estos intentos han sido registrados por la herramienta. A partir de este ataque, se fortalecieron las password de los usuarios ssh en los sistemas en producción de la red siendo más robustas. Por otro lado se configuraron los firewalls para evitar syn flooding al puerto tcp 22.
Se detectaron accesos al servidor proxy-cache desde direcciones públicas con la herramienta Sarg. Esto fue debido a que el servidor se encontraba en modo listen en todas las interfaces de red. Este incidente hizo que se consuma ancho de banda y recursos de hardware de manera inadecuada. Posteriormente se controlaron las directivas de

configuración del servidor proxy y firewall de la red en producción.
En el servidor de correo Postfix se registró el envío de correo de manera masiva a través de una cuenta donde el nombre de usuario de correo y su contraseña eran iguales. Este ataque se detectó a través de Postfix Server Activity Summary, Logwatch e Isoqlog. A partir de este ataque se forzó la actualización de las contraseñas de correo del sistema en producción, con restricciones de cantidad de caracteres y que la misma sea alfanumérica.
Se detectaron correos enviados a través del servidor Qmail donde la dirección con la que se autenticaba el usuario era diferente a la que aparecía en el campo mail from. Esto se resolvió con el parche "From and auth are not the same" para qmail en el sistema en producción. Sin ese parche, un usuario de correo puede "hacerse pasar por otra persona" para el envío de correo electrónico.
El servidor web apache sufrió una denegación de servicio al recibir ataques de synflooding. Además, a través de una incorrecta configuración de php, sufrió un ataque de "Sql Injection" al servidor postgresql. Se detectaron accesos al sistema web publicado en el honeypot de manera no autorizada. Se controlaron las reglas de firewall respecto al servicio web en el sistema de producción, así como tambien las configuracines de los distintos servicios apache con php.
El servidor IIS (Internet Information Server) sufió ataques DoS, por medio de synflooding al puerto 80 del servidor.
Joomla sufrió un ataque a través de un indebido control de datos en un formulario Web. El formulario permitió al atacante subir un archivo .php en lugar de un archivo .jpg. Luego el atacante ejecutó el código php desde el navegador pudiendo editar otros archivos, subir más archivos y observar parámetros de conexión al servidor mysql. El atacante logró realizar un defacement del sitio Web. Todas las actividades quedaron registradas en los logs de acceso del servidor apache. A raíz de este ataque, se consideró insegura la aplicación Joomla para mantenerla en la red de producción.

Discusión

Los resultados obtenidos a través de la presente Investigación permitieron debatir acerca de los mismos, pudiendo destacar en el grupo que los sistemas expuestos a Internet sufrieron ataques casi en forma instantánea, y buscaban vulnerar los distintos servicios instalados, logrando su propósito en varias oportunidades. El servicio que mayor tipo de ataques recibió fue el correo electrónico, que buscaba enviar "Spam" (correo basura).
Por otro lado, se puso de manifiesto, la importancia de utilización de herramientas para la gestión de logs como las que fueron utilizadas en este trabajo, tales como qmailmrtg, isoqlog, nagios, cacti, logwatch, entre otras. Estas herramientas facilitan el estudio del incidente pudiendo realizar un estudio exhaustivo de una manera ágil y sencilla. Además, este tipo de herramientas contribuyen a que los administradores de redes se enteren más rápidamente del incidente, a través de una alerta de correo, un gráfico, etc, que haciéndolo a través de un log de texto o reporte de falla.
Se destaco también la importancia de realizar la customización (personalización) de la configuración de los servicios que las Organizaciones exponen en Internet, ya que en la mayoría de las oportunidades la configuración por defecto es débil o de baja seguridad. Realizar las actualizaciones correspondientes de cada servicio es también una buena práctica, como la de los Sistemas Operativos. Otra práctica recomendada

es realizar antes de cada actualización un backup de los servicios en producción, para contar con una vuelta al estado anterior ante alguna falla. Para ambientes más grandes o críticos otra alternativa sería contar con un ambiente de desarrollo, que sea una réplica del ambiente de producción y realizar las pruebas primero en el de desarrollo, este método conlleva a un mayor costo y esfuerzo en su implementación, pero es más seguro.
También podemos señalar de los estudios realizados, que algunas organizaciones pueden llegar a desconocer a ciencia cierta, si han sido víctimas de ataques informáticos y su verdadero impacto, una de las razones que podemos señalar es que en algunas ocasiones estas vulnerabilidades son explotadas de manera intangible para el usuario del sistema. Estas herramientas que hemos descripto en este documento son solo algunas que permitirían conocer si fueron vulnerados sus sistemas o no.

Conclusión

Con la realización de este proyecto se puso de manifiesto la importancia de la aplicación de buenas prácticas de seguridad en un ambiente informático.
Encontramos en los honeypot una muy buena herramienta para estudiar y aprender sobre la seguridad en redes. El proyecto nos permitió además conocer con mayor exactitud los principales servicios que son víctimas de intentos de ataques, (servicios web y correo electrónico), algunas veces con resultado positivo y otras no, pero sí cabe destacar que es fundamental para cualquier organización que disponga de estos servicios, dedicarles tiempo y esfuerzo en mantener los servicios actualizados y configurados adecuadamente, para prevenir cualquier vulnerabilidad. La caída de un servicio en producción, tiene un alto costo, no solo en términos económicos, sino también el tiempo de improductividad, la reputación de la empresa y la confiabilidad de la misma.
Se lograron determinar y constatar las vulnerabilidades de los servicios testeados así como también cuales son los mecanismos y herramientas utilizadas para explotar dichas vulnerabilidades, esto se llevo a cabo mediante el método de recolección de datos y su posterior análisis.

Los honeypot no pueden ser considerados como un estándar del mercado, como lo pueden ser un Firewall, un router, un antivirus.
La instalación de un honeypot no es tan sencilla como otras herramientas, requieren el conocimiento de conceptos de seguridad informática, redes, etc. También involucra el riesgo y la necesidad de una supervisión intensiva.
Y al mismo tiempo que los honeypot avanzan, los hackers también desarrollan métodos para identificar este tipo de sistemas.
A partir del trabajo actual y observando los resultados se podría trabajar a futuro en los sistemas de Backups, ya que es una de las principales debilidades en la industria, no en la herramienta en sí, sino en su implementación, control y actualización; y permitirá tener un resguardo de toda la información de las Organizaciones en caso de ser víctima de ataques informáticos.

Referencias

[1] - The Honeynet Project, Know Your Enemy: Learning about Security Threats (2nd Edition), Mayo 2004
[2] - L. Spitzner, *"*Honeypots: Catching the Insider Threat*"* Proceedings of the 19th Annual Computer Security Applications Conference, IEEE Computer Society, 2003
[3] - Martin Naedele and Oliver Biderbost. Human-assisted intrusion detection for process control systems, pages 216–225. 2004
[4] - Lance Spitzner, Honeypots: Tracking Hackers, IEEE Computer Society Washington, DC, USA ©2003
[5] Daniel Ramsbrock, Robin Berthier, and Michel Cukier. Profiling attacker behavior following ssh compromises. In Proceedings of

the 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN '07, pages 119–124, Washington, DC, USA, 2007. IEEE Computer Society
[6] Niels Provos and Thorsten Holz. Virtual honeypots: from botnet tracking to intrusion detection. Addison-Wesley Professional, first edition, 2007.
[7] - RFC-2196 Site Security Handbook, por B. Fraser (Editor SEI/CMU), Septiembre 1997
[8] - CISCO SYSTEMS, "CCNA 4 Acceso a la WAN", versión 4.0

Datos de Contacto:

Ing. Norberto Gaspar Cena. Universidad Tecnológica Nacional Facultad Regional Villa María. Av. Universidad 450 – Villa María (Cba) Argentina. ngcena@frvm.utn.edu.ar
Ing. Sebastián Norberto Mussetta.Universidad Tecnológica Nacional Facultad Regional Villa María. Av. Universidad 450 – Villa María (Cba) Argentina.smussetta@frvm.utn.edu.ar
Ing. Fernando Martín Córdoba. Universidad Tecnológica Nacional Facultad Regional Villa María. Av. Universidad 450 – Villa María (Cba) Argentina.mcordoba@frvm.utn.edu.ar
Ing. David Belamate.. Universidad Tecnológica Nacional Facultad Regional Villa María. Av. Universidad 450 – Villa María (Cba) Argentina.dbelamate@frvm.utn.edu.ar
Favro, Ignacio Daniel. Universidad Tecnológica Nacional Facultad Regional Villa María. Av. Universidad 450 – Villa María (Cba) Argentina.idfavro@frvm.utn.edu.ar
Matías Cassani. Universidad Tecnológica Nacional Facultad Regional Villa María. Av. Universidad 450 – Villa María (Cba) Argentina.mcassani@frvm.utn.edu.ar